**WHAT IS CLAIMED IS:**

1. A method of detecting unauthorized actions with respect to encrypted data on a media disk, the media disk including a first portion for pre-recorded content and a second portion for written content, the method comprising:

reading an identifier on the media disk, wherein the identifier includes one or more sections located in one of the first portion for pre-recorded content, the second portion for written content, and both the first portion for pre-recorded content and the second portion for written content;

determining whether the identifier includes a section located in the second portion written content;

comparing the identifier with one or more predetermined types of identifiers for which a section is located in the second portion for written content; and

if the identifier is of a type that is one of the one or more predetermined types of identifiers, detecting an unauthorized action.

2. The method of claim 1 wherein the reading of the identifier on the media disk is during a media disk access operation including one or more of record, play, get play key, copy, open, close and create.

3. The method of claim 2 wherein functionality for the media access disk operation is revoked after detecting the unauthorized action.

4. The method of claim 1 wherein the identifier is one of a plurality of identifiers on the media disk, each identifier being associated with one or more files on the media disk, the files including one of pre-recorded content and written content.

5. The method of claim 1 wherein the predetermined type is an identifier that indicates pre-recorded content and the identifier relates to a location on the media disk for written content.

6. The method of claim 1 wherein the media disk is one of a media disk, a compact disk, a digital video disk, and other digital storage mediums.

7. The method of claim 1 wherein the identifier is pre-recorded on the media disk and the media disk is pre-recorded.

8. The method of claim 1 wherein the predetermined type is an identifier that indicates written content and the identifier relates to a location on the media disk for the written content that is unique to the media disk.

9. The method of claim 1 wherein the identifier is a seed for a key generator, the key generator retrieving one or more keys from a key box, the keys for one or more of unlocking and decrypting files on a media disk.

10. The method of claim 1 wherein the identifier is retrieved from a media disk and used in an engine for a validation function, the validation function performing the comparing the identifier with the one or more predetermined types of identifiers and detecting an unauthorized action.

11. The method of claim 1 wherein the detection of an unauthorized action results in the validation function providing a failure indication.

12. The method of claim 2 wherein detection of an unauthorized action results in revocation of functionality for the media disk access operation.

13. The method of claim 1 wherein the method for detecting unauthorized actions occurs when a media disk is accessed by an engine under a digital rights management protocol.

14. The method of claim 1 wherein the identifier is located on a media disk coupleable to a host, the host being one of an engine, a device that embeds an engine, a third party digital rights management protocol, an application running in an open computing environment, and a clearinghouse server.

15. An apparatus for detecting unauthorized actions with respect to encrypted data on a media disk, the media disk including a first portion for pre-recorded content and a second portion for written content, the apparatus comprising:

means for reading an identifier on the media disk, wherein the identifier includes one or more sections located in one of the first portion for pre-recorded content, the second portion for written content, and both the first portion for pre-recorded content and the second portion for written content;

means for comparing the identifier with one or more predetermined types of identifiers for which a section located in the second portion for written content is not authorized if the identifier includes a section located in the second portion for written content; and

means for detecting an unauthorized action if the identifier is of a type that is one of the one or more predetermined types of identifiers.

16. The apparatus of claim 15 further comprising:

means for determining whether the identifier is a copy of a pre-recorded identifier or an identifier with the combination of pre-recorded data and written data.

17. The apparatus of claim 15 wherein the means for reading of the identifier includes a media disk access component.

18. The apparatus of claim 15 wherein the means for reading the identifier operates during an access operation.

19. The apparatus of claim 15 wherein the identifier is one of a plurality of identifiers on a media disk, each identifier being associated with one or more files on a media disk, the files including one of pre-recorded content and written content.

20. The apparatus of claim 19 wherein at least one of the identifiers is unique to the media disk.

21. The apparatus of claim 15 wherein the identifier is a seed for a cryptographic key box, the key box using the identifier to retrieve one or more keys for unlocking files on a media disk.

22. An engine configured to detect unauthorized actions with respect to encrypted data on a media disk, the media disk including a first portion for pre-recorded content and a second portion for written content, the engine comprising:

a firmware component located on an application specific integrated circuit (ASIC), the firmware component including:

a block configured to read an identifier on the media disk, wherein the identifier includes one or more sections located in one of the first portion for pre-recorded content, the second portion for written content and both the first portion for pre-recorded content and the second portion for written content;

a block configured to compare the identifier with one or more predetermined types of identifiers for which a section located in the second portion for written content is not authorized if the identifier includes a section located in the second portion for written content; and

a block to configured to detect an unauthorized action if the identifier is of a type that is one of the one or more predetermined types of identifiers.

23. A computer program product, the computer program product comprising:

signal bearing media bearing digital information adapted to include programming, the digital information including:

a block configured to read an identifier on the media disk, wherein the identifier includes one or more sections located in one of the first portion for pre-recorded content, the second portion for written content and both the first portion for pre-recorded content and the second portion for written content;

a block configured to compare the identifier with one or more predetermined types of identifiers for which a section located in the second portion for

written content is not authorized if the identifier includes a section located in the second portion for written content; and

a block to configured to detect an unauthorized action if the identifier is of a type that is one of the one or more predetermined types of identifiers.